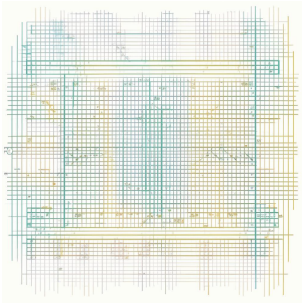
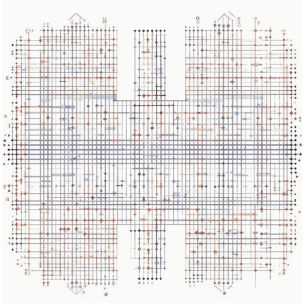
Matrix encode

Вам известно, что система шифрования работает следущим образом: Есть некая секретная матрица

$$X = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{pmatrix}$$, где $n = 256, \forall\ 0 <= i, j <= n, x_{ij} \in \mathbb{Z}_p$, где $p = 277$





Любое сообщение $Text$ это вектор из k элементов поля (то есть вектор длины k элементами которого являются числа от 0 до 276). Шифрование сообщения $Text$ задётся правилами:

- сообщение $Text$ разбивается на блоки $t_1, t_2, \dots$ длинны n чисел и если длина последнего блока меньше, чем n, то он дополняется элементами 0 таким образом, чтобы его длина стала равна n;
- каждый отдельный блок сообщения умножается на матрицу X, согласно правилам матричного умножения $X \cdot t_i^{\downarrow} = s_i^{\downarrow}$, где $i = \overline{1, [\frac{k}{n}]}$, а символ $t^{\downarrow}$ обозначает столбец длины n.

  для простоты обозначим длину сообщения $Text$ в блоках через $l = [\frac{k}{n}]$.
- шифротекст это сообщение вида $s_l, s_{l-1}, \dots s_1$.

Известная информация:

- $n - 1$ пара открытое-шифрованное сообщение состоящее из n чисел.
- n чисел: $\forall i \in \{1, 2, \dots, n\}\ a_i = \sum_{j=1}^{n} x_{ij}$.

Цель:

Расшифровать-дешифровать сообщение M. Сделая это вы получите набор из 256 чисел, после чего вы должны преобразовать числа в строку-флаг по следующему принципу: любое число берется по модулю 256 и после чего переводится в букву по ascii таблице.

Детали:

- Открытые и закодированные сообщения лежат в файлах *open_vectror.txt* и *enocde_vectors.txt* соответственно, по одному сообщению в строке.
- Также значение a_i хранятся в файле *sums.txt*

- Сообщение M хранится в файле *message.txt*